Volume 15, Issue 16   Atari Online News, Etc.   April 19, 2013

Published and Copyright (c) 1999 - 2013
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1516   04/19/13

~ Boston Area Lockdown!   ~ People Are Talking!   ~ Support for CISPA!
~ Anonymous CISPA Protest ~ Bombings Are Scam Bait! ~ Bring Back "Start"!
~ Capcom Halves Forecast! ~ Web Sales Tax Vote Soon ~ Mobile Web Browsing

-* "Aggressive" In-App Purchases *-
-* House Passes the Cybersecurity Bill *-
-* White House Threatens Veto on Cybersecurity *-

=~=~=~=

->From the Editor’s Keyboard   "Saying it like it is!"
""""""""""""""""""""""""""

Boston Strong, Boston Proud! That is the mantra being shouted throughout the city and surrounding areas tonight. On Monday, as most of you are probably aware, there were two explosions at the Boston Marathon. Three spectators were killed, and almost two hundred fans were injured - many critically.

After countless hours of tips and investigation, possible suspects were determined, and a massive manhunt ensued to track them down. On Thursday evening, early Friday morning, the suspects were involved in more horrific terrorist activities; and one suspect was killed. The other managed to escape the immediate area, and another manhunt began.

In the neighboring town of Watertown, the investigation continued throughout the day today. Late this evening, the second suspect was discovered holed up in boat sitting in a neighborhood yard. After an exchange of gunfire, the suspect was taken into custody and brought to an area hospital.

Also, three additional suspects were detained and in custody in a city south of Boston. No information regarding the relation to the Marathon bombings has been publicized yet, but surely any connection will become known soon.

Hopefully, this will be some closure to the week’s events, and some justice will be served for the victims of the events of this week. As a former resident of some of the neighborhoods near where some of these tragedies occurred this week, I feel a sense of community because I recognized some of the areas directly affected. And, as a resident of a town less than 20 miles from Boston, we feel that we’re still a part of that area. As a resident of Massachusetts, I’m elated that all of the various law enforcement agencies were able to work together effectively, keep the public safe, and capture these two suspects (one suspect was ultimately killed). The people of Boston and surrounding areas now have a reason to utter a huge sigh of relief, and might be able to get some much-needed sleep tonight.

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Capcom Halves Forecast, Blames "Excessive Out
sourcing"!
""""""""""""""""""""""""""""   UK Government To Investigate ’Aggressive’ In-

app Purchases

=~=~=~=

->A-ONE’s Game Console Industry News   - The Latest Gaming News!
""""""""""""""""""""""""""""""""""

Capcom Halves Forecast, Blames "Excessive Outsourcing"

Capcom has revised down sales forecasts for its big games of the last year, blaming "excessive outsourcing" for hindering the quality of the finished products, among other factors.

In a note to investors, the company reports that it’s halving its profit forecast due to planned restructuring of the company in a bid to modernise the business.

It explains, "In view of the sudden and significant changes in the operating environment of the digital contents business, Capcom reviewed its business expansion strategy for the sector and restructured its game development organization."

An accompanying presentation reveals that this will mean "the discontinuation of development of titles" that have yet to be announced, including overseas outsourced projects that are "no more compatible with the current business strategy."

The other factor behind the downcast of profits is revised sales figures for the likes of Resident Evil 6, Monster Hunter and DmC: Devil May Cry. The company now predicts it’ll shift 4.9 million copies of Resi 6; when the game first launched, this number was 7 million. For DmC, the number’s gone down to 1.15 million when it was originally 2 million.

Three reasons were given for the disappointing sales: a "delayed response to the expanding digital contents market"; "insufficient coordination between the marketing and the game development divisions in overseas markets"; and, most interestingly, a "decline in quality due to excessive outsourcing".

While we don’t know whether Monster Hunter 4 will be released in the west, the company still has a number of exciting projects due to release this financial year including Remember Me and Deep Down.

UK Government To Investigate ’Aggressive’ In-app Purchases

The UK Government will be examining whether free to download apps are putting unfair pressure on kids to pay up for additional content within the game through in-app purchases.

Office of Fair Trading, UK, will be carrying out the investigation of games that include commercially aggressive in-app purchases after a number of cases have been reported whereby parents have incurred huge bills after their kids have spent huge amounts on in-app purchases.

February, this year, saw 5-year old Danny Kitchen spending £1700 on in-app purchases while playing the otherwise free Zombies vs. Ninjas game. Similar was the case with Cameron Crossan unwittingly spent over £3700 on in-app purchases. We believe they could have averted it if they would have turned off in-app purchases in their iOS devices.

OFT wants to hear from parents who believe or have otherwise dealt with games / apps that push children to buy in-game content. Generally there are objects such as gems or coins within games, which if bought, will allow kids to advance through the games faster. Such tactics may lure kids to go ahead with in-app purchases.

Cavendish Elithorn, OFT’s Senior Director, said "We are concerned that children and their parents could be subject to unfair pressure to purchase when they are playing games they thought were free, but which can actually run up substantial costs." The government is not looking to ban in-app purchases but it wants to be sure that the game developers are complying with the relevant laws.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

White House Threatens Veto of House Cybersecurity Bill

The White House on Tuesday threatened to veto a House of Representatives bill aimed at improving U.S. cybersecurity, citing among other things concerns about privacy protections.

In a repeat of last year’s events, the Obama administration issued a new veto threat on the cybersecurity bill co-authored by House Intelligence Committee Chairman Mike Rogers, saying it needed to better protect private information and gave too much liability protection to companies.

"The Administration still seeks additional improvements and if the bill, as currently crafted, were presented to the president, his senior advisors would recommend that he veto the bill," the statement of administration policy said on Tuesday.

The House is expected to vote on the bill later this week.

To try to gain support of the White House and in an effort to appease concerns of civil liberties groups, Intelligence Committee leaders made some changes to the wording of the bill, which is very similar to a bill passed by the House in 2012 that focused on helping companies and the

U.S. government share information on cyber threats.

Changes this year include a provision preventing companies from using information they receive for anything but cybersecurity purposes. It also includes added roles for privacy and civil liberties oversight.

"The Committee adopted several amendments to (the bill) in a good faith effort to incorporate some of the administration’s important substantive concerns. However (it) ... still does not address these fundamental priorities adequately," said Caitlin Hayden, a National Security Council spokeswoman.

In 2012, legislation authored by Rogers and Democrat Dutch Ruppersberger passed the House but died in the Democratic-controlled Senate after President Barack Obama similarly threatened to veto it.

The White House has sought a more comprehensive piece of legislation that would also set minimum security standards for critical companies.

Michelle Richardson of the American Civil Liberties Union on Tuesday called the veto threat "completely justified" and said it did not bode well for the bill’s future in the Senate.

Rogers’ office did not immediately comment.

House Passes Cybersecurity Bill As Privacy Concerns Linger

The House of Representatives passed legislation on Thursday designed to help companies and the government share information on cyber threats, though concerns linger about the amount of protection the bill offers for private information.

This is the second go-around for the Cyber Intelligence Sharing and Protection Act after it passed the House last year but stalled in the Senate after President Barack Obama threatened to veto it over privacy concerns.

The bill drew support from House Democrats, passing on a bipartisan vote of 288-127, although the White House repeated its veto threat on Tuesday if further civil liberties protections are not added.

Some lawmakers and privacy activists worry that the legislation would allow the government to monitor citizens’ private information and companies to misuse it.

U.S. authorities have recently elevated the exposure to Internet hacks and theft of digital data to the list of top threats to national security and the economy.

Though thousands of companies have long been losing data to hackers in China and elsewhere, the number of parties publicly admitting such loss has been growing. The bill’s supporters say a new law is needed to let the government share threat information with entities that don’t have security clearances.

"If you want to take a shot across China’s bow, this is the answer," said the House bill’s Republican co-author and Intelligence Committee Chairman

Mike Rogers.

While groups such as the American Civil Liberties Union are displeased, House Democratic Whip Steny Hoyer called the new version of the bill "a significant improvement from what was passed last year."

Senator Jay Rockefeller, the West Virginia Democrat who chairs the Senate Commerce Committee, said he will work with Republican Senator John Thune of South Dakota and leaders of other committees to bring cyber legislation to a vote in the Senate as soon as possible.

"Today’s action in the House is important, even if CISPA’s privacy protections are insufficient," Rockefeller said in a statement. "There is too much at stake - our economic and national security - for Congress to fail to act."

House Intelligence Committee leaders have made refinements and endorsed several amendments to the bill to try to put to rest some of the privacy concerns. In particular, these specify that the Department of Homeland Security and the Department of Justice rather than any military agencies would be the clearinghouses of the digital data to be exchanged - to "give it a civilian face," as Rogers put it.

"We felt very strongly that it had to be civil," said the bill’s Democratic co-author Dutch Ruppersberger of Maryland. "If you don’t have security, you don’t have privacy."

House Democratic leader Nancy Pelosi reflected concerns shared by the White House and many civil liberties groups, that the bill did not do enough to ensure that companies, in sharing cyber threat data with the government and each other, strip out any personal data of private citizens.

"They can just ship the whole kit and caboodle and we’re saying minimize what is relevant to our national security," Pelosi said. "The rest is none of the government’s business."

Still, the future of cybersecurity legislation in the Senate remains unclear, given Obama’s veto threat and the lingering concerns of many privacy-focused lawmakers and groups.

Late Thursday, the Obama administration reiterated that cybersecurity is a top priority and said it would work with both parties to build on the House legislation and get a bill through the Senate.

"While CISPA has been improved in each of the administration’s priority areas since its introduction this year, the bill does not yet adequately address our fundamental concerns," said Laura Lucas, a spokeswoman for the White House’s National Security Council. "We are hopeful that continued bipartisan, bicameral collaboration to incorporate our core priorities will produce cybersecurity legislation that addresses these critical issues and that the president can sign into law."

Industry groups that supported the measure welcomed the House’s action.

Backers included the wireless group CTIA, the U.S. Chamber of Commerce and TechNet, which represents big technology companies such as Google Inc, Apple Inc, Yahoo! Inc and Cisco Systems Inc.

Boston Residents on Lockdown Share Fear on Twitter, Facebook

As Boston has been put on lockdown as authorities conduct a "massive manhunt" to find the second Boston Marathon bombing suspect, residents of the city have taken to Facebook and Twitter to share with friends and family that while they are frightened, they are safe and remaining indoors.

At 7:19 a.m. this morning Juliana Hatfield (@julianahatfield) tweeted a photo of a sign that was left on her door by police in the City of Cambridge. She also told her followers that "I'm fine - thanks for the concern, everyone   i wasn't planning on leaving my apartment today anyway - now i have more."

i fell asleep to the sound of helicopters overhead and woke up to this on my front door-whoa twitter.com/julianahatfiel

  Juliana Hatfield (@julianahatfield) April 19, 2013

"Residents of Watertown asked to stay indoors," the Boston Police Department tweeted. "Do not answer door unless instructed by a police officer." Public transportation has been suspended and authorities told people at closed stops and stations to go home. The situation is scary, to say the least. In fact, #scared was a trending term on Twitter in Boston this morning.

I wish I could say that I'm not scared, but I've never been more terrified in my life.

  Kenny Benjamin (@KennyBenjamin) April 19, 2013

I shouldn't be scared to live in my own city #Boston

  Eliza Gulbis (@ElizaGabrielle) April 19, 2013

I'm seriously scared right now. Way to close to my house. (2blcks)Afraid of explosives. Everything. Be safe people #watertown #bostonstrong

  Barry (@barrygagne) April 19, 2013

I miss the days when we stayed home because it snowed. #Boston

  Carl (@CMorriss87) April 19, 2013

Many others, who weren't even in Boston, also shared their fear for the people living in the city.

And like we saw on Monday after the bombing, the non-Boston community, has been sharing their support and prayers for the community.

#PRAYERS for Boston & This World.

  Steve Smith (@steve21smith) April 19, 2013

Wow. thinking about Boston and the surrounding areas. Sending love and prayers.

  Sara Bareilles (@SaraBareilles) April 19, 2013

Boston Bombings Used as Malware Scam Bait

Just hours after the Boston Marathon bombings Monday (April 15), scammers were already using the tragedy to fuel their malware campaigns, according to a study by Romanian anti-virus firm Bitdefender.

The study found that the words "marathon," "Boston" and "explosion" found their way into the subject headers of one out of every five spam messages in the hours and days following the event.

The use of news events to spread malware is nothing new for scammers. Just last month, scammers used the news of the pope’s installment as bait for email victims. Emails containing links to malware-laden sites were circulated with subject lines such as "New Pope Sued for Not Wearing Seatbelt in Popemobile."

But this week s spam strikes a more somber note. With subject headers such as "Aftermath to Explosion at Boston Marathon" and "Boston Explosion Caught on Video," these emails aim to ensnare those looking for more information about the attacks.

According to Bitdefender’s Hot for Security blog, the emails contain links to malicious websites using URLs ending with "news.html" and "boston.html."

How to Avoid Boston-Bombing Online Scams

When clicked, the links direct users to a seemingly innocuous YouTube page displaying videos of the bombings. But after a short delay, an executable file is activated and the malware installs itself on victims’ computers.

Bitdefender identified the malware as Trojan.GenericKDZ.14575, a component of the infamous RedKit browser exploit pack   the same malware that recently infected visitors to the NBC website.

The Trojan is a password stealer that can grab users account passwords directly from their browsers. The malware also monitors network traffic of infected computers and may be used to steal Bitcoin wallets, send emails and download other malware.

As TechNewsDaily reported in the hours following the Boston bombings, Internet users need to remain alert in the wake of major news events.

Be wary of unsolicited emails, even those you receive from friends. If you want to donate to victims, do so only through charity organizations you know and trust.

Last but not least, make sure your anti-virus software warns your Web browser about malicious links.

Tech Group Representing Google, Yahoo Backs CISPA

A trade association that represents Google, Yahoo, Cisco and Oracle has come out in support of a controversial cybersecurity bill that is slated to be voted on in the House next week.

In a letter sent to the leaders of the House Intelligence panel on Wednesday, TechNet CEO Rey Ramsey said the cybersecurity bill addresses the need for industry and government to be able to send and receive information about cyber threats to one another in real time. He also commended the Intelligence panel leaders for taking steps to address privacy concerns with their bill, the Cyber Intelligence Sharing and Protection Act (CISPA), but also said the trade group looked forward to continuing talks on "further privacy protections."

"We commend the committee for providing liability protections to companies participating in voluntary information-sharing and applaud the committee’s efforts to work with a wide range of stakeholders to address issues such as strengthening privacy protections," Ramsey writes. "As the legislative process unfolds, we look forward to continuing the dialogue with you and your colleagues on further privacy protections, including discussions on the role of a civilian interface for information sharing."

Privacy and civil liberties groups have been pushing for the bill to be amended so it would put a civilian agency, like the Department of Homeland Security, in charge of information-sharing efforts between industry and the government. Privacy advocates have argued that a civilian agency should be in charge of receiving cyber threat data, such as malicious source code, from companies first before passing it on to other intelligence agencies, such as the National Security Agency.

The bill would allow companies to share cyber threat data directly with the NSA, along with other government agencies.

While privacy groups have staunchly opposed CISPA, it has received backing from several industry groups, such as the U.S. Chamber of Commerce and Information Technology Industry Council.

Several high-profile tech executives sit on TechNet’s executive council, including Yahoo CEO Marissa Mayer, Google Executive Chairman Eric Schmidt, Oracle President Safra Catz and venture capitalist John Doerr. A list of the members on TechNet’s executive council are printed on the letter that the trade group sent to House Intelligence Chairman Mike Rogers (R-Mich.) and Dutch Ruppersberger (D-Md.).

CISPA is aimed at encouraging industry and the government to share information about malicious source code and other online threats with each other in real time, so companies and government agencies can take steps to thwart cyberattacks.

The bill is intended to remove the legal hurdles that discourage companies from sharing cyber threat data with the government. Companies have said they are hesitant to share threat information with the government because it may result in legal action against them.

CISPA passed the House Intelligence panel on a 18-2 vote on Wednesday and is headed to the House floor for a vote next week. Reps. Adam Schiff (D-Calif.) and Jan Schakowsky (D-Ill.) voted against the measure, citing privacy concerns.

The White House issued a veto threat against CISPA last year, in part, because of concerns that it lacked sufficient privacy protections for people’s information online.

Following Wednesday’s markup, a White House spokeswoman said the changes adopted to CISPA "reflect a good faith effort" to address some of the substantive concerns it has with the measure, but don’t go far enough to solve its "fundamental" issues with the bill.

Anonymous Calls for Internet Blackout Day To Protest CISPA

The Cyber Intelligence Sharing and Protection Act (CISPA), which passed the House of Representatives this week, has drawn a lot of criticism from activist groups such as the Electronic Frontier Foundation for potentially undermining users online privacy. In particular, the EFF has said that the bill gives Internet companies the right to monitor user actions and share data   including potentially sensitive user data   with the government without a warrant and also overrides existing privacy law, and grants broad immunities to participating companies.

Hacker collective Anonymous this week called for a massive online protest against CISPA to occur on April 22nd through an Internet Blackout Day by asking web developers and website owners to go dark and to also display a message as to why you are going dark, and encourage others to do the same. The group s call for an online blackout day echoes a similar protest that occurred last year against the Stop Online Piracy Act (SOPA) in which Reddit and Wikipedia both went dark to protest the bill while Google blacked out its famous Google doodle to symbolize its opposition.

Senate Edges Closer To Vote on Internet Sales Tax

Legislation giving states the power to compel retailers outside their borders to collect online sales taxes, a touchy subject for Internet merchants, is likely to move forward in the Senate next week.

Senate Majority Leader Harry Reid on Thursday filed a motion in support of the measure. Currently, states rely on consumers to self-report, which they rarely do.

If approved, the change would be a win for brick-and-mortar stores like Wal-Mart Stores Inc., the world’s biggest retailer, which backs the legislation.

At the moment, states can only require online merchants with physical stores or affiliates within their borders to collect sales tax, giving online-only retailers such as Amazon.com Inc a price advantage in many markets.

As a results of Reid’s motion, the Senate was expected to vote on Monday on whether to end debate and move the measure forward. A vote on the legislation could come later in the week. Backers say they have the 60 votes needed to end debate.

Momentum has been building since 75 of 100 senators last month voted for a nonbinding version of the bill. The road ahead for the measure is bumpier in the House of Representatives, where some Republicans view it as a tax hike.

One House sponsor, conservative Representative Steve Womack, has been lobbying fellow Republicans to support the measure, according to an aide.

But Republican Bob Goodlatte, chairman of the Judiciary Committee, where the bill would have to go through, said he is skeptical.

"While it attempts to make tax collection simpler, it still has a long way to go," Goodlatte said.

Womack is from Arkansas, home of Walmart. Amazon.com also supports the measure, but others including eBay Inc oppose it.

Microsoft Told To Bring Back Start Button

While Windows 8 has a lot going for it, it s also proven to be a very polarizing operating system that many users have criticized for departing too much from earlier versions. The most common complaint lobbed at Windows 8 is that it lacks the classic Start button that Microsoft users have long relied on as a central navigation tool. But with rumors percolating that Microsoft is considering dialing back some of the changes it made to Windows with the next major update to the operating system, Forrester analyst J.P. Gownder is encouraging the company to go all-out and bring back the Start button as a nod to users constructive criticisms.

Numerous Start Button emulators with names like StartIsBack, Pokki, and StartMenu are proliferating   and many of them are free, Gownder writes. Yet I&O departments can t support users easily with these emulators and would prefer a Start Button that s simply part of the OS.

Gownder also addresses potential concerns that Microsoft may have about selling its vision of touch-enabled PCs short by bringing back the Start button. In essence, Gownder thinks users will happily accept the return of the Start button and will be thankful to the company for taking their concerns into account.

During the period when the Windows Store s modern UI apps continue to grow in number and sophistication, Windows 8 users need to have the strongest possible Desktop Mode experience, he writes. Empowering users with familiar tools wouldn t be a sign of surrender, but rather a sign that Microsoft listens to its customers.

Mobile Web Browsing Not Great, Says Mozilla CEO

Chances are you spend most of your time in apps on your phone, while the web browser takes a backseat. Mozilla, the maker of the popular Firefox browser, acknowledges that the industry has fallen short in improving mobile web browsers.

"We haven’t done a great job [on mobile browsing]. I’m expecting someone will do a Apple on the whole browsing experience," Mozilla CEO Gary Kovacs said at the All Things D: Dive Into Mobile conference today in New York City.

Kovacs is referring to, of course, how Apple revolutionized or changed the entire phone business with the iPhone. He added that he anticipates that at some point the mobile browser will provide an "entirely different experience," rather than just a shrunken down version of the desktop browser.

What that experience might look like Kovacs didn’t detail, but Mozilla is betting big on the browser being at the center of the mobile phone experience. The company announced its Firefox OS earlier this year; the operating system for phones is based on its Firefox browser. The phones that will run the Firefox OS software will launch in select countries this June. While they will launch in Venezuela, Poland, Brazil, Portugal and others this year, they will come to the U.S. in 2014.

The company has already partnered with Sprint.

Currently Mozilla offers a mobile version of its Firefox browser for Android. It’s not available on the iPhone, Kovacs said, because "iOS has a policy where you have to use their web engine. Our web engine is very different." The company does not want to adjust that, he explained.

Kovacs announced today that he would be stepping down as the CEO of Mozilla this year. "I learned in college that you don’t want to stay at a party too long," he said at the conference. "It’s time for me to move on to other things."

If It Ain’t Broke, Don’t Fix It: Ancient Computers in Use Today

It s easy to wax nostalgic about old technology - to remember fondly our first Apple IIe or marvel at the old mainframes that ran on punched cards. But no one in their right mind would use those outdated, underpowered dinosaurs to run a contemporary business, let alone a modern weapons system, right?

Wrong!

While much of the tech world views a two-year-old smartphone as hopelessly obsolete, large swaths of our transportation and military infrastructure, some modern businesses, and even a few computer programmers rely daily on technology that hasn t been updated for decades.

If you ve recently bought a MetroCard for the New York City Subway or taken money from certain older ATMs, for instance, your transaction was made possible by IBM s OS/2, an operating system that debuted 25 years ago and faded out soon after.

A recent federal review found that the U.S. Secret Service uses a mainframe computer system from the 1980s. That system apparently works only 60 percent of the time. Here s hoping that uptime statistics are better for the ancient minicomputers used by the U.S. Department of Defense for the Minuteman Intercontinental Ballistic Missile system, Navy submarines, fighter jets, and other weapons programs. Those systems, according to the consultants who help keep them going, will likely be used until at least the middle of this century.

Here are a few stories of the computers that time forgot, and the people and institutions that stubbornly hold on to them.

Sparkler Filters of Conroe, Texas, prides itself on being a leader in the world of chemical process filtration. If you buy an automatic nutsche filter from them, though, they ll enter your transaction on a computer that dates from 1948.

Sparkler s IBM 402 is not a traditional computer, but an automated electromechanical tabulator that can be programmed (or more accurately, wired) to print out certain results based on values encoded into stacks of 80-column Hollerith-type punched cards.

Companies traditionally used the 402 for accounting, since the machine could take a long list of numbers, add them up, and print a detailed written report. In a sense, you could consider it a 3000-pound spreadsheet machine. That’s exactly how Sparkler Filters uses its IBM 402, which could very well be the last fully operational 402 on the planet. As it has for over half a century, the firm still runs all of its accounting work (payroll, sales, and inventory) through the IBM 402. The machine prints out reports on wide, tractor-fed paper.

Of course, before the data goes into the 402, it must first be encoded into stacks of cards. A large IBM 029 key-punch machine - which resembles a monstrous typewriter built into a desk - handles that task.

Carl Kracklauer, whose father founded Sparkler Filters in 1927, usually types the data onto the punch cards. The company sticks with the 402 because it’s a known entity: Staffers know how to use it, and they have over 60 years of company accounting records formatted for the device.

The key punch isn’t the only massive accessory in Sparkler’s arsenal. The 402 also links to an IBM 514 Reproducing Punch, which has been broken for three years. When it works properly, the 514 spits out punched "summary cards," which typically contain the output of the 402’s operation (such as sum totals) for later reuse. Sparkler stores all of its punched data cards - thousands and thousands of them - in stacks of boxes.

The company also possesses dozens of 402 programs in the form of IBM plugboards. Computer programming in the 1940s commonly involved arranging hundreds of individual wires in a way that would likely drive a modern software engineer insane. In the 402’s case, a spaghetti-like pattern of wires attached to hundreds of connectors on each plugboard determines the operation of the machine, and different plugboards can be pulled out and replaced as if they were interchangeable software disks. So you might insert one plugboard for handling, say, accounts receivable, and a different one for inventory management.

Sparkler s 402 is a such a significant computing relic that the Computer History Museum in Mountain View, California, sent a delegation to the company last year to try and convince its executives to move to a more modern accounting system and donate the 402 to the museum. That will someday be an appropriate resting place for the 402, but as long as it still does its duty, the Texas company has no problem keeping its digital dinosaur living a little while longer.

When you see reports about the small, remote-controlled drones that the military uses to gather intelligence and target enemies in Pakistan and Afghanistan, it s easy to assume that all our weaponry is equally modern. Some significant weapons systems that our military depends on today, though, run on technology that dates back, in some instances, to the

Vietnam War era.

The U.S. Navy s ship-based radar systems and Britain s Atomic Weapons Establishment, which maintains that country s nuclear warheads, use PDP minicomputers manufactured in the 1970s by Digital Equipment Corporation (DEC). Another user of the PDP is Airbus, the French jetliner manufacturer.

The PDP was among the second wave of mainframes called minicomputers because they were only the size of a couple of refrigerators instead of big enough to fill a room.

The F-15 and F-18 fighters, the Hawk missile systems, parts of the U.S. Navy submarine fleet, and Navy fighter test systems on aircraft carriers use DEC s VAX minicomputers from the 1980s for various purposes, according to Lynda Jones of The Logical Company in Cottage Grove, Oregon, which helps keep these antiquated systems functioning.

Because of their critical nature, many of these systems will be in continuous service long into the future, perhaps to the middle of this century. For instance, the Minuteman ICBM program, which uses DEC VAX systems for testing, recently received funding that will keep it going until 2030.

"These legacy systems are integrated into multibillion dollar systems as control or test systems," Jones says. Replacing these old systems with modern machines, she explains, would cost millions of dollars and could potentially disrupt national security.

As it turns out, replacing those systems with modern hardware designed to work like the antiquated components is a decidedly less risky venture. Jones’ company is one of many that create systems to simulate older DEC minicomputers using newer, smaller, and less power-hungry electronic parts. The replacement computers emulate the exact functionality of the original hardware - and run the same vintage software - so it appears to the rest of the system as if nothing has changed.

That’s important because most of Logical’s customers are defense corporations refreshing old weapons technology under contract with the U.S. Department of Defense. "There are thousands of DEC systems in use for military applications around the world," says Jones, "including PDPs from the 1970s, VAXes from the 1980s, and Alphas from the 1990s."

The United States developed many fighter jet and missile systems during the Cold War era using DEC hardware for test and control functions, says Jones, because the company’s minicomputers were among the very first general-purpose machines that did not require water cooling and could be used in harsh environments.

The biggest problem with maintaining such ancient computer systems is that the original technicians who knew how to configure and maintain them have long since retired or passed away, so no one is left with the knowledge required to fix them if they break.

Even if someone does know how to fix them, finding replacement parts can be tricky. Stanley Quayle, a computer emulation consultant, has seen contractors desperate to find the parts they need. "I have a prospective customer supporting a U.S. missile defense system that is buying parts on eBay," says Quayle. "Any parts they do find are as old or older than their system," meaning they re sometimes no more reliable than the pieces they replace.

Lots of people fell in love with the Apple IIe when it was released in 1983. It supported a wide variety of software and hardware, it was reliable, and its seven internal expansion slots made it extremely flexible.

For Kevin Huffman, who owns and operates Huffman Industrial Warehouse in Eden, North Carolina, that love has never waned. His firm stores and ships out goods for companies that rent his warehouse space, and he regularly uses his vintage Apple IIe to track inventory and keep accounts.

Huffman got started with the Apple II line in college and later bought two identical Apple IIe systems from his brother-in-law in the mid-1980s, one of which he uses today. (He keeps the other unit as an emergency backup.)

Huffman’s Apple IIe setup is nothing fancy, but it is fully stocked. It’s equipped with 128 kilobytes of RAM, the standard 1MHz 6502 CPU, and AppleSoft BASIC in ROM. It contains five expansion cards: a printer card, two disk interface cards, a serial port card, and an 80-column video card. For peripherals, he uses an Apple DuoDisk unit, a 10-inch amber video monitor, and a trusty workhorse of a printer - a Star NP-10 that "is still going strong at 26-plus years old," he says.

Huffman runs an application suite on the Apple IIe called "The Business Accountant," first published by Manzanita Software in 1984. Of the six applications in the suite, he uses five: General Ledger, Accounts Payable, Accounts Receivable, Inventory, and Payroll. All of his data resides on the once-standard 5.25-inch floppy disks, but he’s not worried about data security: "I back up the floppies with a program called Copy II+."

Huffman uses a modern PC for word processing, email and Web browsing, but he’s reluctant to move away from his trusty Apple IIe for accounting work.

"I still use the machine because it is so simple to use, I know the software, and I can still update the tax tables manually." He adds, "The only glitch in the entire system is that it does not recognize the year 2000, so all my printed financial reports say 1912. But on the invoices, checks, and other forms, it prints in the 11/14/12 format."

He’s even tried emulating the Apple IIe and his favorite software on a modern machine, but to him, the full experience matters. "I thought about changing over to a more modern system, but there is nothing to be gained. As the old saying goes, ’If it ain’t broke, don’t fix it.’"

Few vintage computers inspire as much active devotion as the Tandy Color Computer 3, first introduced in 1986. The CoCo 3 (as it is affectionately called by its fans) never sold as many units as home computers from Atari or Commodore, but that engendered an even stronger loyalty in its users.

The CoCo 3 marked the end of a well-received line of Color Computer products from RadioShack, which launched the first model in 1980. The third model in the series turned out to be an impressive swan song, adding support for 512KB of memory and implementing advanced graphics and sound enhancements - all while retaining backward compatibility with pre-CoCo 3 software.

It’s understandable, then, that some folks refuse to let go of their CoCo 3 units for either work or play. One such loyal user, John Kowalski, a former console game developer, still considers his CoCo 3 an indispensable tool.

"I turn it on, type in a quick program to do something I need done, and let it run to get the results," says Kowalski. "I think of it as my personal assistant - sometimes I program it to do tedious or repetitive tasks like automated document reformatting, and I can continue working while it works beside me."

Kowalski began his journey in CoCo-land with a Color Computer 2 in 1984. He traded up to the CoCo 3 in 1986 and stuck with the platform through the years, performing various hardware upgrades (upping the system RAM to 2MB and overclocking the 6809 CPU to a blistering 3.5MHz) along the way.

When Kowalski was programming console video games at Crystal Dynamics in the mid-to-late 1990s, his vintage CoCo 3 played a prominent role. "Every game I worked on had at least some data in it created on the CoCo," he says. Titles like Namco Museum 50th Anniversary and Tron 2.0: Killer App benefited from the vintage machine, which Kowalski used as if it were a powerful programmable scientific calculator.

For an original title like Tron 2.0 for the Xbox, Kowalski used the CoCo 3 to test 3D techniques used in the game. "Many of the data sets used by the 3D engine were generated on the CoCo, like the tables for calculating depth and perspective in the 3D view, and the data for fish-eye reduction of the view," he says. "The texture map graphics used in the game were also translated into program data by a conversion tool I wrote on the CoCo."

If speed wasn’t an issue, Kowalski would quickly type up a program in the CoCo’s built-in BASIC interpreter. In the cases that involved large amounts of graphics or sound data, he would turn to assembly language.

The latter technique proved quite handy when working on Namco Museum or Atari Anniversary, which both contained reworkings of classic 1980s arcade games. Kowalski used the CoCo to extract, convert, and edit graphics data from the original arcade ROMs into formats a PlayStation 2 console could use. He also used the CoCo to translate vintage arcade source code and clean up sound samples used in the games.

With such an old machine, you might think it would be hard to export the working data to a more modern PC, but Kowalski has found no such problems. For years, he swapped standard 5.25-inch disks between his CoCo 3 and a Windows PC. Today, he simply connects a serial port between the CoCo and a PC, with the PC acting as a virtual disk drive emulator.

Kowalski says his current job designing electronics hardware doesn’t call for much data generation, so he doesn t use the CoCo as frequently. But he hasn’t retired the classic machine; Kowalski keeps the 25-year-old PC on his main computer desk, ready to be called back into service at a moment’s notice.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.